

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)Information associated with pengwm2019@gmail.com that is
stored at premises controlled by Google, LLC, 1600
Amphitheatre Parkway, Mountain View, CA 94043

Case No.

2:22 mj-386

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE THE ATTACHED AFFIDAVIT IN SUPPORT OF THIS APPLICATION, AND ATTACHMENT A THERETO IN PARTICULAR, ALL OF WHICH IS INCORPORATED HEREIN BY REFERENCE.

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

SEE THE ATTACHED AFFIDAVIT IN SUPPORT OF THIS APPLICATION, AND ATTACHMENT B THERETO IN PARTICULAR, ALL OF WHICH IS INCORPORATED HEREIN BY REFERENCE.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. 1956(h)	Money laundering conspiracy
31 U.S.C. 5324	Structuring transactions to evade reporting requirement prohibited

The application is based on these facts:

See attached affidavit incorporated herein by reference.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn to before me and signed in my presence.

Date:

6-1-22

City and state: Columbus, Ohio

Jordan Flexman

Applicant's signature

Jordan Flexman, SA/FBI

Printed name and title

Chelsey M. Vascura

Judge's signature

Chelsey M. Vascura, U.S. Magistrate Judge

Printed name and title



**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION**

In the Matter of the Search of:

pengwm2019@gmail.com

UNDER SEAL

No.

**AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT FOR
STORED ELECTRONIC COMMUNICATIONS**

I, Special Agent Jordan Flexman, being duly sworn, hereby depose and state:

I. INTRODUCTION AND SUMMARY OF PROBABLE CAUSE

1. As set forth in detail below, a federal law enforcement investigation is being conducted into possible violations of federal criminal laws by Qiaoping NIE (NIE). In particular, Your Affiant submits that the facts herein establish probable cause to believe NIE is in violation of 31 U.S.C. § 5324(a)–(c) (Structuring) and 18 U.S.C. § 1956(h) (Money Laundering Conspiracy) (collectively referred to as the SUBJECT OFFENSES).

2. Relevant here, I make this Affidavit in support of an Application for a search warrant for information contained in pengwm2019@gmail.com (SUBJECT ACCOUNT) that is stored at premises controlled by Google LLC (Google or the Provider), an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043, believing evidence, fruits, and instrumentalities of the SUBJECT OFFENSES will be found within the

SUBJECT ACCOUNT. This Affidavit is made in support of an Application for a search warrant under the SUBJECT OFFENSES to require Google to disclose to the United States copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

3. The SUBJECT ACCOUNT is as follows: The email account pengwm2019@gmail.com (SUBJECT ACCOUNT), affiliated with NIE, which is maintained at premises controlled by Google, a company headquartered in Mountain View, California.

4. This Affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

II. AGENT BACKGROUND

5. I have been employed as a Special Agent of the Federal Bureau of Investigation (FBI) since September 2019, and I am currently assigned to the Cincinnati Division, Columbus Resident Agency, as a member of the Counterintelligence Squad. I am responsible for investigating, among other crimes, the theft or bribery concerning programs receiving federal funds, as well as wire fraud, money laundering, and structuring. I have received both formal and informal training in the detection and investigation of said offenses. As a result of my training and experience, I am familiar with the federal laws relating to structuring and money laundering. I have participated in various investigations, including with a foreign counterintelligence nexus. As a federal agent, I am authorized to investigate violations of the laws of the United States. I have

personally participated in the investigation described herein. I have reviewed the relevant documents and reports during the course of this investigation. The statements contained in this Affidavit are based on my own observations, document reviews, and reliable information provided to me by other law enforcement officials. Because this Affidavit is being submitted for the limited purpose of establishing probable cause to search the property described herein, I have not included each and every fact learned during the course of this investigation. Rather, I have set forth those facts that I believe are necessary to establish probable cause for the search warrant sought. Where actions, conversations, and statements of others are related, they are related in part, except where otherwise indicated.

6. Based on my training and experience and the facts set forth in this Affidavit, there is probable cause to believe that violations of 31 U.S.C. § 5324 (a)–(c) and 18 U.S.C. § 1956(h) have been committed by NIE. There is also probable cause to believe that fruits, evidence, and instrumentalities of these crimes in the form of electronic communications are located as described in Attachments A and B at the email service provider.

III. THE PROVIDERS AND THE SUBJECT ACCOUNTS

7. I make this Affidavit in support of an Application for a search warrant to Google (“Google”) pursuant to Title 18, U.S.C. § 2703, for all content and other information associated with the following: The email account pengwm2019@gmail.com (SUBJECT ACCOUNT), created on or about 03/11/2019, maintained at premises controlled by Google, a company headquartered in Mountain View, California.

8. I have learned through Federal Grand Jury Subpoenas that the SUBJECT ACCOUNT was utilized by NIE as part of her contact information regarding her JP Morgan Chase bank account, her TD Ameritrade brokerage account, and her Zelle digital payment account.

9. On or about 11/15/2021, a 2703(d) Order was served to Google for subscriber information and transactional records regarding the SUBJECT ACCOUNT. Based on the 2703(d) Order, the account was created on or about 03/11/2019, from IP address 75.118.2.131, which resolves near NIE's residence. Another IP address identified from the 2703(d) Order, 219.228.136.20, resulted back to the China Education and Research Network Center. The given name, family name, and date of birth used to create the SUBJECT ACCOUNT resolve back to Weiming Peng, date of birth 3/12/1969. Per open source database checks, the name and date of birth listed, with regard to the SUBJECT ACCOUNT, do not exist and appear fabricated. However, the name "Peng" is listed as NIE's mother's surname on NIE's DS-160 (part of her visa application).

10. NIE also used the aforementioned fabricated name when creating a payment profile associated with the above-described Google account. Per review of the payment profile, the address given, 1603 Waltham Road, Upper Arlington, OH 43221, resolves back to NIE's address. In addition, the payment profile includes a Chase credit card (Mastercard x8812), which is registered to NIE's name and ties to the SUBJECT ACCOUNT.

11. **Services and Providers.** In my training and experience, I have learned the following about Google (or the Provider):

- a. The Provider offers email services to the public. In particular, the Provider allows subscribers to maintain e-mail accounts under a variety of domain names, such as gmail.com, like the SUBJECT ACCOUNT. A subscriber using the Provider's services can access his or her email account from any computer connected to the internet.
- b. The Provider maintains the following records and information with respect to every subscriber account:
 - i. **Email contents.** In general, any email (which can include attachments such as documents, images, and videos) sent to or from a subscriber's account, or stored in draft form in the account, is maintained on the Providers' servers unless and until the subscriber deletes the email. If the subscriber does not delete the email, it can remain on the
 - ii. **Providers' computers indefinitely.** Even if the subscriber deletes the email, it may continue to be available on the Providers' servers for a certain period of time.
 - iii. **Stored Files.** In addition to emails, a Google subscriber can also store files with the provider, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.
 - iv. **Subscriber and billing information.** The Provider collects and maintains (typically unverified) identifying information about their subscribers, such as the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account user's location, communications, or pattern of conduct. Based on my training and experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.
 - v. **Transactional information.** In my training and experience, the Provider also typically retains certain transactional information about the creation and the use of each account on its system. This information can include the date on which the account was created, the length of service, records

of login (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), other log files that reflect usage of the account, and the methods used to connect to the account (such as logging into the account through the Providers' websites). In addition, email providers often have records of the Internet Protocol (IP address) used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

- vi. **Customer correspondence.** In my experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. The Providers also typically maintain records of any customer service contacts with or about the subscriber, including any inquiries or complaints concerning the subscriber's account. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.
- vii. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish probable cause and prove each element or, alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant of a residence. For example, email communications, contact lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at the relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example as described below, email providers typically log the IP addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may

further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Stored electronic data might also provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

- viii. Google Plus (stylized as Google+) is an internet-based social network owned and operated by Google. The following paragraphs detail the features and functions associated with Google Plus social networking accounts:
 - a. **User profile:** A Google Plus user profile is a publicly visible account of a user that is attached to many Google properties. The user profile includes basic social networking services like a profile photo, about section, background photo, cover photo, previous work and school history, interests, places lived, and an area to post status updates.
 - b. **Circles:** Circles enables a user to organize people into groups or lists for sharing across various Google products and services. Organization of Circles is done through a "drag and drop" interface. Once a Circle is created, a Google Plus user can share specific private content to only that circle.
 - c. **Stream:** Within the Stream section, Google Plus users see updates from those in their Circles. There is an input box which allows users to create a post. Along with the text field there are icons to upload and share photos and videos.
 - d. **Privacy:** The privacy setting allows Google Plus users to disclose certain information to the Circles of their choice. Users can also see their profile visitors.
- ix. Google Plus also retains IP logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Google Plus, including information about the type of action, the date and time of the action, and the user IP and IP address associated with the action. For example, if a user views a Google Plus profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

- x. Social networking providers like Google Plus typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Google Plus users may communicate directly with Google about issues relating to their account(s), such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Google Plus typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communication.
- xi. Therefore, the computers of Google are likely to contain all the material just described, including stored electronic communications and information concerning subscriber and their use of Google Plus, such as account access information, transaction information, and account Application.
- xii. Google Drive is a file storage and synchronization service developed by Google. Google Drive allows users to store files on their servers, synchronize their devices and share files. Google Drive offers users 15 gigabytes of free storage with virtually unlimited storage space through an optional paid plan. Digital files uploaded can be up to 5 terabytes in size.
- xiii. Google Drive users have the ability to upload any digital file to Google Drive for data retention and data backup. Google Drive users have the ability to access their content from their Google Drive account from any device connected to the internet, including computers, tablets, Android smartphones or iPhones.
- xiv. Based on my training and experience, Gmail, Google Plus, and Google Drive, as well as other Google products, can all be backed up and synchronized with each other. The back-up and synchronization process creates additional copies of digital files in multiple locations for ease of access and to secure data from accidental deletion.
- xv. This Application seeks a warrant to search all responsive records and information under the control of Google, which is a provider subject to the jurisdiction of this court, regardless of where Google has chosen to store such information. The United States intends to require the disclosure pursuant to the request warrant of the contents of wire or electronic communications and any records or other information pertaining to the

customers or subscribers if such communication, record, or other information is within Google's possession, custody, or control regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

IX. JURISDICTION AND AUTHORITY TO ISSUE WARRANTS

12. Pursuant to 18 U.S.C. § 2703(a), (b)(1)(A) & (c)(1)(A), the Government may require a provider of an electronic communications service or remote computing service, such as the Provider, to disclose all stored content and all non-content records or other information pertaining to a subscriber, by obtaining a warrant issued using the procedures described in the Federal Rules of Criminal Procedure 41.

13. A search warrant under § 2703 may be issued by "any district court of the United States (including a magistrate judge of such a court)" that (i) "has jurisdiction over the offense being investigated," 18 U.S.C. § 2711(3)(A)(i); (ii) "is in ... a district in which the provider ... is located or in which the wire or electronic communications, records, or other information are stored," 18 U.S.C. § 2711(3)(A)(ii); or (iii) "is acting on a request for foreign assistance pursuant to 18 U.S.C. § 3512," 18 U.S.C. § 2711(3)(A)(iii).

14. When the Government obtains records under § 2703 pursuant to a search warrant, the Government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2) & (3). Additionally, the Government may obtain an order precluding the Providers from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize an investigation. 18 U.S.C. § 2705(b).

15. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. *See* 18 U.S.C. § 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

IV. STATUTES AND REGULATIONS

16. I am advised that 31 U.S.C. § 5324 criminalizes what is known as “structuring”—that is, manipulating financial transactions to evade currency reporting requirements.

17. I am advised that 18 U.S.C. § 1956(h) criminalizes engaging in a money laundering conspiracy—that is, conspiring with another to conduct or attempt to conduct a financial transaction knowing that the property involved in the transaction represents the proceeds of some form of unlawful activity, either to promote the carrying on of the unlawful activity or conceal the nature of the proceeds of the unlawful activity.

V. FACTS ESTABLISHING PROBABLE CAUSE

A. Background: NIE Financial Accounts

18. NIE, a Chinese citizen and U.S. J1 visa holder, is a Visiting Scholar at The Ohio State University (OSU) in the Department of East Asian Languages and Literature. Her listed education is a PhD from the Department of Chinese Language and Literature, Fudan University, People’s Republic of China. According to her OSU webpage, retrieved on or about 02/02/2022, NIE’s area of expertise is Chinese pedagogy. NIE has held this position at OSU teaching graduate students since January 2019. When NIE applied for a U.S. visa she accessed a U.S. Government web-based system called Student Exchange Visitor Information System (SEVIS). SEVIS

maintains information on nonimmigrant students and exchange visitors in the United States. SEVIS implements Section 641 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, which requires the Department of Homeland Security to collect current information from nonimmigrant students and exchange visitors continually during their course of stay in the United States. Per SEVIS record details, NIE submitted an application for a J1 visa on or about 09/28/2018 to come to the United States and declared she had financial support for \$93,000 from "Other Organizations." Applicants for U.S. visas have four options to choose from when declaring their financial support: Financial Support from Exchange Visitor's Government, Binational Commission, Other Organizations, and Personal Funds. On or about 10/30/2020, NIE was interviewed by an agent of the U.S. Department of Homeland Security, Homeland Security Investigations. NIE gave the agent a different answer than when she applied for her J1 visa. Rather than saying that she had financial support from "Other Organizations," she informed the agent that her salary while in the United States has been paid by the Chinese Government, specifically the Chinese Department of Education and the Chinese International Languages Department Exchange.

19. As laid out in detail in this Affidavit, through FBI investigation and per Grand Jury Subpoenas to U.S. Bank and TD Ameritrade, it was identified that Allen D. Wilson, owner of Creative Production Solutions, Inc, a software IT business consulting agency, is a close financial associate of NIE's.

20. The investigation has indicated the following U.S. financial accounts in NIE's name:

- a. Fifth Third Bank: x1616 and x3190

b. U.S. Bank: x2487

c. TD Ameritrade: x6749

d. JP Morgan Chase Bank: x6799, x2017, x2339, x2583, and x8812

21. The following bank accounts are in Allen WILSON's name:

a. TD Ameritrade: x4237

b. Huntington National Bank: x2973

22. Over the course of the investigation, multiple Grand Jury Subpoenas have been served to different entities to include, Fifth Third Bank, The Ohio State University, JPMorgan Chase Bank, Western Union, TD Ameritrade, US Bank, and Zelle.

23. Per a Grand Jury Subpoena issued to Fifth Third Bank, on or about 08/14/2019, two bank accounts were established in NIE's name, one ending in x1616 and another ending in x3190. The following information is associated with the Fifth Third Bank Accounts: phone number (614) 816-3734; home address 1603 Waltham Rd., Upper Arlington, OH, 43221; and social security number ending in 4514. NIE provided the same phone number to The Ohio State University when she filled out her Hire Data Worksheet with The Ohio State University. The social security number ending in 4514 and address at 1603 Waltham Rd. is also the same number and address on file with the Ohio Bureau of Motor Vehicles.

24. Per a Grand Jury Subpoena issued to U.S. Bank, on or about 12/02/2020, a bank account ending in x2487 was established in NIE's name. The following information is associated with the U.S. Bank account: home address 1603 Waltham Rd., Upper Arlington, OH 43221, date of birth 07/12/1966, and social security number ending in x4514. The social security number

ending in 4514, date of birth of 07/12/1966, and address at 1603 Waltham Rd. are the same number, date of birth, and address on file with the Ohio Bureau of Motor Vehicles.

25. Per a Grand Jury Subpoena issued to TD Ameritrade, on or about 06/17/2020, an individual brokerage account ending in x6749 was established in NIE's name. The following information is associated with the TD Ameritrade account: email address pengwm2019@gmail.com (SUBJECT ACCOUNT); phone number (614) 816-3734; home address 1603 Waltham Rd., Columbus, OH 43221; and social security number ending in x4514. NIE provided the same phone number to The Ohio State University when she filled out her Hire Data Worksheet with The Ohio State University. The social security number ending in x4514 and address at 1603 Waltham Rd. are the same number and address on file with the Ohio Bureau of Motor Vehicles.

26. Per a Grand Jury Subpoena issued to JP Morgan Chase Bank, on or about 12/12/2018, two bank accounts were established in NIE's name, one ending in x6799 and another ending in x2017. The following information is associated with accounts x6799 and x2017: 1603 Waltham Rd, Upper Arlington, OH 43221-3863, date of birth 07/12/1966, and NIE's passport number x8148. On or about 08/06/2020, another account ending in x2339 was established in NIE's name with JP Morgan Chase Bank. The following information is associated with accounts x2339: 1603 Waltham Rd., Upper Arlington, OH 43221-3863, phone number (614) 816-3734, date of birth 07/12/1966, NIE's passport number x8148, social security number x4514. Additionally, on or about 09/21/2019, JP Morgan Chase Bank issued a credit card ending in x2583 in NIE's name. The following information is associated with account x2583: 1603 Waltham, Upper Arlington,

OH 43221-3863, date of birth 07/12/1966, phone number 614-816-3734, email address qiaoping2012@126.com. Finally, on or about 11/21/20, JP Morgan Chase Bank issued a credit card ending in x8812 in NIE's name. The following information is associated with the JP Morgan Chase Bank account x8812: home address 1603 Waltham Rd., Upper Arlington, OH 43221, social security number x4514, date of birth 7/12/1966, cell phone number 614-816-3734, email address pengwm2019@gmail.com (SUBJECT ACCOUNT).

27. On or about 09/28/2018, NIE applied to the US Department of State for a J1 visa to travel to the US and provided email address qiaoping2012@126.com. The same email address was used to establish the JP Morgan Chase Bank credit card ending in x2583.

28. Per a Grand Jury Subpoena issued to TD Ameritrade, an individual brokerage account ending in x4237 was affiliated with Allen Wilson. The following information is associated with the x4237 TD Ameritrade account: social security number ending in x5077; 2933 Blendon Woods Blvd., Columbus, OH 43231; telephone number (614) 284-1300; and email address ohiorider565@hotmail.com (WILSON's EMAIL).

B. Evidence of Structuring; Corresponding Email Activity Related to the SUBJECT ACCOUNT

29. Based upon training and experience, Your Affiant is aware that the term "structuring" refers to the manipulating of transactions to evade currency-reporting requirements. For example, a given individual might know that a cash deposit of over \$10,000 or more will trigger a banker's obligation to file a report; and, in order to avoid the report, that individual will then proceed to deposit a sum in excess of \$10,000 through multiple deposits that are each under

\$10,000. Your Affiant is further aware that such conduct implicates 18 U.S.C. 31 U.S.C. § 5324(a)-(c), one of the SUBJECT OFFENSES.

30. Your Affiant respectfully submits that, based upon training and experience, the below-described financial activity is indicative of structuring, and is further consistent with money laundering. Moreover, as described further below, and based upon training and experience, Your Affiant submits that the SUBJECT ACCOUNT was engaged in communications during the periods of the below-described activity in a manner that relates to the SUBJECT OFFENSES.

31. A 2703d order to Gmail revealed that, from on or about 08/03/2019 through on or about 08/08/2019, the SUBJECT ACCOUNT corresponded with email address fenglee5142@gmail.com approximately eight times. The investigation has indicated that, during time periods relevant to the above-described date range, NIE engaged in the following financial activity, which, based upon training and experience, is indicative of structuring:

- a. On or about 08/05/2019, seven money orders with sequential serial numbers from 17684819568 to 17684819574, each with face amounts of \$1,000, for a total of \$7,000, were purchased in the name of NIE at Kroger #942 in Columbus, OH. The money orders were made payable to NIE. These money orders were then deposited on or about 08/06/2019 into JP Morgan Chase Bank account ending in x6799 belonging to NIE.
- b. On or about 08/08/2019, seven money orders with sequential serial numbers from 17681601235 to 17681601241, each with face amounts of \$1,000, for a total of \$7000, were purchased in the name of NIE at Kroger #942 in Columbus, OH. The

money orders were made payable to NIE. These money orders were then deposited into an account belonging to NIE.

- c. Additionally, on or about 8/12/2019, seven money orders with sequential numbers from 17681601315-17681601321, each with face amounts of \$1,000, for a total of \$7,000, were purchased in the name of NIE at Kroger #942 in Columbus, OH. The money orders were made payable to NIE. These money orders were then deposited into an account belonging to NIE.

32. As mentioned above, the investigation has indicated that Allen D. WILSON is a financial associate of NIE'S. By way of general background, during time periods relevant to the investigation and this Affidavit, WILSON has been the beneficiary of Automated Clearing House and Pay a Person payments from NIE's personal accounts. These payments from NIE's personal accounts were derived from cash deposits, for which the true source of the funds is unknown, as well as money orders that were purchased by NIE and deposited into her account. As a result of the financial activities between NIE and WILSON, via their respective TD Ameritrade accounts, TD Ameritrade applied account restrictions on both WILSON's and NIE's accounts.

33. Moreover, a 2703d order to Gmail revealed that, from on or about 8/8/2020 through on or about 8/18/2020, the SUBJECT ACCOUNT corresponded with WILSON's email account approximately eight times. The investigation has indicated that, during time periods relevant to the above-described date range, NIE engaged in the following financial activity:

- a. On or about 8/10/2020, two money orders with sequential serial numbers of 19118226308 and 19118226309, with face amounts of \$1,000.00, all totaling

\$2,000.00, were purchased in the name of NIE at the same location, KROGER #942, in Columbus, Ohio. The money orders were made payable to NIE. Grand Jury Subpoenas to JP Morgan Chase Bank showed these money orders were then deposited on 8/10/2020 by NIE to her JP Morgan Chase Bank account number x6799.

- b. Per a Grand Jury Subpoena issued to JP Morgan Chase Bank, on or about 8/11/2020, two money orders with sequential serial numbers of 19118226350 and 19118226351, with face amounts of \$1,000.00, totaling \$2,000.00, were purchased by NIE at the same location, KROGER #942, in COLUMBUS, OH. The money orders were made payable to NIE. The money orders were then deposited by NIE at/to JP Morgan Chase Bank into Account Number x6799 in the name of NIE.
- c. Per a Grand Jury Subpoena issued to JP Morgan Chase Bank, on or about 8/12/2020, two money orders with sequential serial numbers from 19118226362 and 19118226363, with face amounts of \$1,000.00, totaling \$2,000.00, were purchased by NIE at the same location, KROGER #942, in COLUMBUS, OH. The money orders were made payable to NIE.
- d. On or about 8/13/2020, money orders with serial numbers 19118226380 and 19118226381 with face amounts of \$1,000.00, totaling \$2,000.00, were purchased by NIE at the same location, KROGER #942, in COLUMBUS, OH. The money orders were made payable to NIE.

- e. On or about 8/14/2020, money orders with serial numbers of 19168347601 and 19168347602, with face amount of \$1,000.00, totaling \$2,000.00, were purchased by NIE at the same location, KROGER #942, in COLUMBUS, OH. The money orders were made payable to NIE. The money orders purchased on 8/12/2020, 8/13/2020, and 8/14/2020 were deposited by NIE on 8/14/2020 at/to JP MORGAN CHASE BANK into ACCOUNT NUMBER x6799 in the name of NIE.

C. Additional Evidence of Structuring and Money Laundering Related to the SUBJECT ACCOUNT

34. As stated above, the investigation has revealed the following accounts relevant to this Affidavit:

- a. Huntington National Bank x2973, in the name of Allen Wilson (HNB x2973)
- b. TD Ameritrade x4237, in the name of Allen Wilson (TD x4237)
- c. TD Ameritrade x6749, in the name of Qiaoping NIE (TD x6749)

35. Per a Grand Jury Subpoena to Huntington National Bank, from on or about 12/18/2020 through on or about 4/07/2021, HNB x2973 (WILSON) received a total of nine international wire transfers from "ZHAI YU JIA MR," "1/ZHAI YI JIA," and "MERITCO SERVICES CO., LTD," all totaling \$369,930. Three Chinese Banks were utilized in making these transfers: China Merchants Bank x1010; HSBC Hong Kong x5838; IE HSBC Bank China A/C x9406. Over the same period, \$369,970 was transferred from HNB x2973 (WILSON) to TD x4237 (WILSON), and then internally transferred to TD x6749 (NIE). Notably, TD account x6749 (NIE) appears to have then returned \$25,984.84 to x4237 (WILSON). Below is a more detailed

accounting of the above-described transactions; Your Affiant respectfully submits that, based upon training and experience, the below-described financial activity is indicative of structuring, and is further consistent with money laundering:

- a. Per Grand Jury Subpoenas to Huntington National Bank and TD Ameritrade, on or about 12/18/20, HNB x2973 (WILSON) received one incoming wire transfer from 1/Zhai Yu Jia in the amount totaling \$29,985.00. On or about 12/21/2020, HNB x2973 (WILSON) received one incoming wire transfer from 1/Zhai Yu Jia in the amount totaling \$29,985.00. On or about 12/21/20, a transfer was made from HNB x2973 (WILSON) to TD x4237 (WILSON) in the amount of \$29,985. On or about, 12/22/20, \$29,985 was transferred from HNB x2973 (WILSON) to TD x4237 (WILSON). On or about, 12/28/20, TD x6749 (NIE) received two internal transfers from TD x4237 (WILSON) totaling \$59,970. Further, between on or about 12/16/2020 and 12/17/2020, the SUBJECT ACCOUNT corresponded with WILSON's email account approximately five times.
- b. Per Grand Jury Subpoenas to Huntington National Bank and TD Ameritrade, on or about 1/21/21, HNB x2973 (WILSON) received one incoming wire transfer from Meritco Services Co LTD in the amount of \$50,000. On or about 1/22/21, TD x4237 (WILSON) received payment from HNB x2973 (WILSON) for \$50,000. On or about 1/28/21, TD x6749 (NIE) received an internal transfer from TD x4237 (WILSON) for \$50,000. Further, between on or about 1/18/2021 and on or about

1/23/2021, the SUBJECT ACCOUNT corresponded with WILSON's email account approximately five times.

- c. Per Grand Jury Subpoena to Huntington National Bank and TD Ameritrade, on or about 2/1/2021, HNB x2973 (WILSON) received one incoming wire transfer from Meritco Services Co LTD in the amount of \$50,000.00. On or about 2/2/2021, a transfer of \$50,000.00 was made through an ACH payment from HNB x2973 (WILSON) to TD x4237 (WILSON). On or about 2/08/2021, \$50,000.00 was internally transferred from TD x4237 (WILSON) to TD x6749 (NIE).
- d. Per Grand Jury Subpoenas to Huntington National Bank and TD Ameritrade, on or about 2/3/21, HNB x2973 (WILSON) received one incoming wire transfer from Meritco Services Co LTD in the amount of \$50,000. On 2/5/21, TD x4237 (WILSON) received ACH payment from HNB x2973 (WILSON) for \$50,000. On or about 2/11/21, TD x6749 (NIE) received an internal transfer from TD x4237 (WILSON) for \$50,000. Further, between on or about January 31, 2021, and on or about February 11, 2021, the SUBJECT ACCOUNT corresponded with WILSON's email account approximately eight times.
- e. Per Grand Jury Subpoenas to Huntington National Bank and TD Ameritrade, on or about 3/18/21, HNB x2973 (WILSON) received one incoming wire transfer from Zhai Yu Jia Mr in the amount of \$29,980. On or about 3/19/21, HNB x2973 (WILSON) received one incoming wire transfer from Zhai Yu Jia Mr for \$29,980. On or about 3/22/21, TD x4237 (WILSON) received ACH payment from

HNB x2973 (WILSON) for \$60,000. On or about 3/25/21, TD x6749 (NIE) received internal transfer from TD x4237 (WILSON) for \$60,000.

- f. Per Grand Jury Subpoena to Huntington National Bank and TD Ameritrade on or about 3/23/21, HNB x2973 (WILSON) received one incoming wire transfer from Meritco Services Co LTD in the amount of \$40,000. On or about 3/26/21, TD x4237 (WILSON) received ACH payment from HNB x2973 (WILSON) for \$40,000. On or about 4/5/21, TD x6749 (NIE) received an internal transfer from TD x4237 (WILSON) for \$40,000. Further, between on or about March 15, 2021, and March 26, 2021, the SUBJECT ACCOUNT corresponded with WILSON's email approximately 11 times.
- g. Per Grand Jury Subpoenas to Huntington National Bank and TD Ameritrade, on or about 4/7/21, HNB x2973 (WILSON) received one incoming wire transfer from Meritco Services Co LTD in the amount of \$60,000. On or about 4/9/21, TD x4237 (WILSON) received ACH payment from HNB x2973 (WILSON) for \$60,000. On or about 4/20/21, TD x6749 (NIE) received an internal transfer from TD x4237 (WILSON) for \$55,000. On or about 4/21/21, TD x6749 (NIE) received an internal transfer from TD x4237 (WILSON) for \$5,000. Further, between or about 3/29/2021 and 4/23/2021, the SUBJECT ACCOUNT corresponded with WILSON's email account approximately 23 times.
- h. Per Grand Jury Subpoenas to Huntington National Bank and TD Ameritrade, between on or about 2/8/2021 to on or about 4/1/2021, \$25,984.84 was internally

transferred from TD x6749 (NIE) to TD x2973 (WILSON) across 3 transactions. On or about 2/8/21, TD x4237 (WILSON) received an internal transfer from TD x6749 (NIE) for \$1,184.84. On or about 3/2/21, TD x4237 (WILSON) received an internal transfer from TD x6749 (NIE) for \$5,900. On or about 4/1/21, TD x4237 (WILSON) received an internal transfer from TD x6749 (NIE) for \$18,900.

36. In addition, as a result of the aforementioned internal transfers between WILSON and NIE through TD Ameritrade, on or about 8/9/2021, TD Ameritrade contacted both NIE and WILSON and stated the following, in relevant part: "After reviewing the activity in your account, it has become imperative to request that you discontinue the use of your brokerage account for conducting fund transfers, and ask that future fund disbursements be returned to the account of origin. While this may not have been your intention and recent activity may not be representative of your full account history, we felt it was important to bring this to your attention in order to maintain the valued relationship we have with you. TD Ameritrade discourages our clients from using their accounts primarily as 'pass-through' accounts to facilitate the transfer of funds. TD Ameritrade must take measures to ensure the functionality is used appropriately; therefore, account restrictions have been placed on your account."

37. Based upon the foregoing, there is probable cause to believe that information stored on the Providers' servers associated with the SUBJECT ACCOUNT will contain evidence, fruits, and instrumentalities of the SUBJECT OFFENSES, as more fully described in Attachment B.

38. In particular, based upon training and experience and the factual allegations detailed in this Affidavit, Your Affiant submits that the SUBJECT ACCOUNT is likely to contain, among other things, the following information:


- a. Evidence of the identity of the user of the SUBJECT ACCOUNT;
- b. Evidence regarding whether NIE, using the SUBJECT ACCOUNT, conspired with others or acted on behalf of others to structure their deposits;
- c. Evidence regarding whether NIE, and others, purposefully tried to evade reporting requirements;
- d. Evidence of whether NIE, and others, knew of the reporting requirements and acted to avoid them;
- e. Evidence of any criminal proceeds, if applicable, from the structured deposits; and
- f. Evidence connected to a specified unlawful activity.

D. CONCLUSION

39. In conclusion, Your Affiant submits that the evidence stated herein establishes probable cause to believe that NIE has violated U.S. law regarding Title 31 U.S.C. § 5324 (structuring transactions to evade reporting requirements), and Title 18 U.S.C. § 1956(h) (money laundering conspiracy). Your Affiant further submits that there is also probable cause to believe that evidence, fruits, and instrumentalities of this crime will be found on the premises of Google, as described above. Based on the foregoing, I respectfully request that the Court issue the warrant sought to search the location described in Attachment A and seize those items set forth in Attachment B, attached hereto and incorporated herein, pursuant to the applicable provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) (for contents) and § 2703(c)(1)(A) (for records and other information), and the relevant provisions of Federal Rule of Criminal Procedure 41.

IX. REQUEST FOR SEALING

40. I further request that the Court order that all papers in support of this Application, including the Affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.


Jordan Flexman
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me this 1 day of June 2022.



United States Magistrate Judge
United States District Court
Southern District of Ohio

ATTACHMENT A
Property to be Searched

This warrant applies to information associated with pengwm2019@gmail.com, the SUBJECT ACCOUNT, which is stored at premises owned, maintained, or operated by Google, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043.

ATTACHMENT B
Particular Things to be Seized

I. Information to be disclosed by Google

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, Inc., regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Google, Inc., or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google is required to disclose the following information to the United States for each account or identifier listed in Attachment A. Such information should include the below-described content of the SUBJECT ACCOUNT from February 1, 2019, to the present.

1. The contents of all emails, opened or unopened, associated with the SUBJECT ACCOUNT, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
2. Any deleted emails, including any information described in subparagraph "1." above;
3. All records or other information regarding the identification of the SUBJECT ACCOUNT, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
4. All available IP history related to the SUBJECT ACCOUNT;
5. The types of service utilized;

6. All records or other information stored by an individual using the Google accounts, including address books, contact and buddy lists, calendar data, pictures, videos and files. In addition, please provide the photos and videos in their original file format, including EXIF information;
7. All records pertaining to communications between Google and any person regarding the account, including contacts with support services and records of actions taken;
8. All Google chat archives stored on servers controlled by Google;
9. All privacy settings and other account settings; and
10. All records pertaining to any Circles in which the Google accounts listed in Attachment A participated, including communications and content shared with other individuals within such Circles, the other individuals within those Circles, and the account/subscriber information of the other individuals within those Circles.

II. Information to be seized by the United States

All information described above in Section I, including correspondence, records, documents, photographs, videos, electronic mail, chat logs, and electronic messages, that constitutes evidence of a crime, contraband, fruits of crime, or other items illegally possessed, or property designed for use, intended for use, or used in committing violations of 31 U.S.C. § 5324(a)–(c) (Structuring) and 18 U.S.C. § 1956(h) (Money Laundering Conspiracy), including, for each account or identifier listed on Attachment A, information pertaining to the following matters, including attempting and conspiring to engage in the following matters:

1. Credit card and other financial information including but not limited to bills and payment records.
2. The identity of the person(s) who created or used the SUBJECT ACCOUNT, including records that help reveal the whereabouts of such person(s).

3. Evidence indicating how and when the SUBJECT ACCOUNT was accessed or used to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the email account owner.
4. Passwords and encryption keys, and other access information that may be necessary to access the account(s) or identifier(s) listed in Attachment B and other associated accounts.
5. The identity of the person(s) who communicated with the users of the SUBJECT ACCOUNT about matters relating to structuring, money laundering, crimes related to the money laundering, other financial crimes/illegal practices, and/or circumventing United States financial laws and regulations.
6. Records and information related to the SUBJECT OFFENSES.
7. Records and information relating to NIE's state of mind as it relates to the SUBJECT OFFENSES.
8. Records and information relating to the involvement of any other individuals in the SUBJECT OFFENSES.
9. Records and information relating to NIE's involvement with the China Merchants Bank and HSBC Hong Kong.
10. Records and information relating to any financial transaction or other movement of any things of value, to or from NIE, as well as any documents, including but not limited to Forms 1099 and Forms W-2, filed with any taxing authority in connection with those transactions.
11. Records and information relating to any financial transaction or other movement of any things of value, to or from any company with which NIE is affiliated, as well as any documents, including but not limited to Forms 1099 and Forms W-2, filed with any taxing authority in connection with those transactions.